AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims

1. (Previously Presented) A method of communicating data securely within a wireless communications network, comprising the steps of:

maintaining a database server and a separate authentication server;

storing information and an associated data record within said database server, said information adapted to being accessed by a mobile station, said information having been encrypted using a data access key;

maintaining said data access key within said authentication server;

transmitting, by said mobile station, a first authentication request to said authentication server;

receiving said first authentication request at said authentication server from said mobile station;

providing a first key from said authentication server to said mobile station in response to said first authentication request;

receiving a second authentication request at said authentication server from said database server, said second authentication request further including said first key provided by said authentication server to said mobile station and a particular data identifying said information to which said mobile station is requesting access;

determining at said authentication server as to whether said mobile station has authority to access said particular database record; and

in response to an affirmative determination,

instructing said database server to provide information associated with said requested database record to said mobile station; and

providing by said authentication server to said mobile station a second key enabling said mobile station to decrypt said information received from said database server using said second key.

2. (Original) The method of Claim 1 wherein said step of providing said first key to said mobile station further comprises the step of providing a time out period for said first key to said mobile station.

3. (Original) The method of Claim 1 wherein said information stored in said database server is encrypted using a data access key and said second key is generated from said data access key and said first key.

4. (Original) The method of Claim 1 wherein said step of instructing said database server to provide information to said mobile station further comprises the step of providing said database server with a third key wherein said third key is used by said database server to further encrypt said information.

5. (Original) The method of Claim 4 wherein said information stored in said database server is encrypted using a data access key and wherein said third key is generated from said data access key and said first key and said second key is generated from said data access key, said first key and said third key.

6. (Original) The method of Claim 1 further comprising the steps of:

receiving a third authentication request from said database server requesting authorization to update said particular database record by said mobile station;

determining whether said mobile station has authority to update said database record; and

in response to an affirmative determination,

instructing said database server to allow said mobile station to update information associated with said database record; and

providing said mobile station with said second key enabling said mobile station to encrypt any information to be transmitted over to the database server to be updated at said database record.

7. (Original) The method of Claim 1 wherein said information stored in said

database record is encrypted using a data access key and said second key provided to said mobile station is generated from said data access key and said first key.

8. (Previously Presented) A method of storing and communicating data securely within a mobile telecommunications network wherein said mobile telecommunications network provides wireless service to a wireless device and further includes an authentication server and a separate database server, comprising the steps of:

storing particular information within said database server wherein said information and an associated data record is stored encrypted using a first encryption key;

communicating, by said wireless device, separately with said authentication server and said database server;

receiving a request from said wireless device to access said information within said database server;

in response to said request, transmitting an authentication request from said database server to said authentication server;

receiving authentication approval, by said database server, from said authentication server regarding said wireless device for said information;

further providing, by said authentication server a decryption key to said wireless device; and

providing, by said database server, said requested information encrypted to said wireless device wherein said wireless device decrypts said information using said decryption key provided by said authentication server.

9. (Previously Presented) The method of Claim 8 wherein said step of receiving said authentication approval from said authentication server further comprises the steps of:

receiving, by said database server, a second encryption key from said authentication server;

encrypting, by said database server, said stored information using said second

encryption key; and

providing said encrypted information to said wireless device.

10. (Original) The method of Claim 8 wherein said step of receiving said request from said wireless device to access said information further comprises the step of receiving a session key generated by said authentication server from said wireless device.

11. (Original) The method of Claim 10 wherein said step of transmitting said request to said authentication server further comprises the step of including said session key within said request.

12. (Original) The method of Claim 8 further comprising the steps of:

receiving a second request from said wireless device to store particular information within said database server;

transmitting a second authentication request to said authentication server;

receiving second authentication approval from said authentication server instructing said database server to allow said wireless device to update said database server with said requested information;

receiving said particular information from said wireless device wherein said information being encrypted using a particular encryption key; and

storing said encrypted information within said database server.

13 - 18. (Cancelled)

19. (Currently Amended) A mobile communications network for storing and communicating data securely with a wireless device, comprising:

a database server;

an authentication server;

a means for storing particular information within said database server, said information adapted to being accessed by said wireless device, wherein said

information is stored encrypted using a first encryption key;

a means for receiving a request for information from said wireless device to access said stored information within said database server;

a means for transmitting an authentication request from said database server to said authentication server in response to said request for information;

a means for receiving authentication approval from said authentication server regarding said wireless device for said requested information wherein said authentication server further providing an decryption key to said wireless device; and

a means for providing said requested information encrypted to said wireless device wherein said wireless device decrypts said information using said decryption key provided by said authentication server.

20. (Previously Presented) The mobile communications network of claim 19 wherein said means of said database server for receiving said authentication approval from said authentication server further comprises:

means for receiving a second encryption key from said authentication server;

means for encrypting said stored information using said second encryption key; and

means for providing said encrypted information to said wireless device.

21. (Previously Presented) The mobile communications network of Claim 19 wherein said request from said wireless device to access said information further comprises a session key generated by said authentication server from said wireless device.

22. (Previously Presented) The mobile communications network of Claim 21 wherein said request to said authentication server further comprises said session key received from said wireless device.